OIPE
MAR 1 5 2004
PATENT & TRADEMARK OFFICE

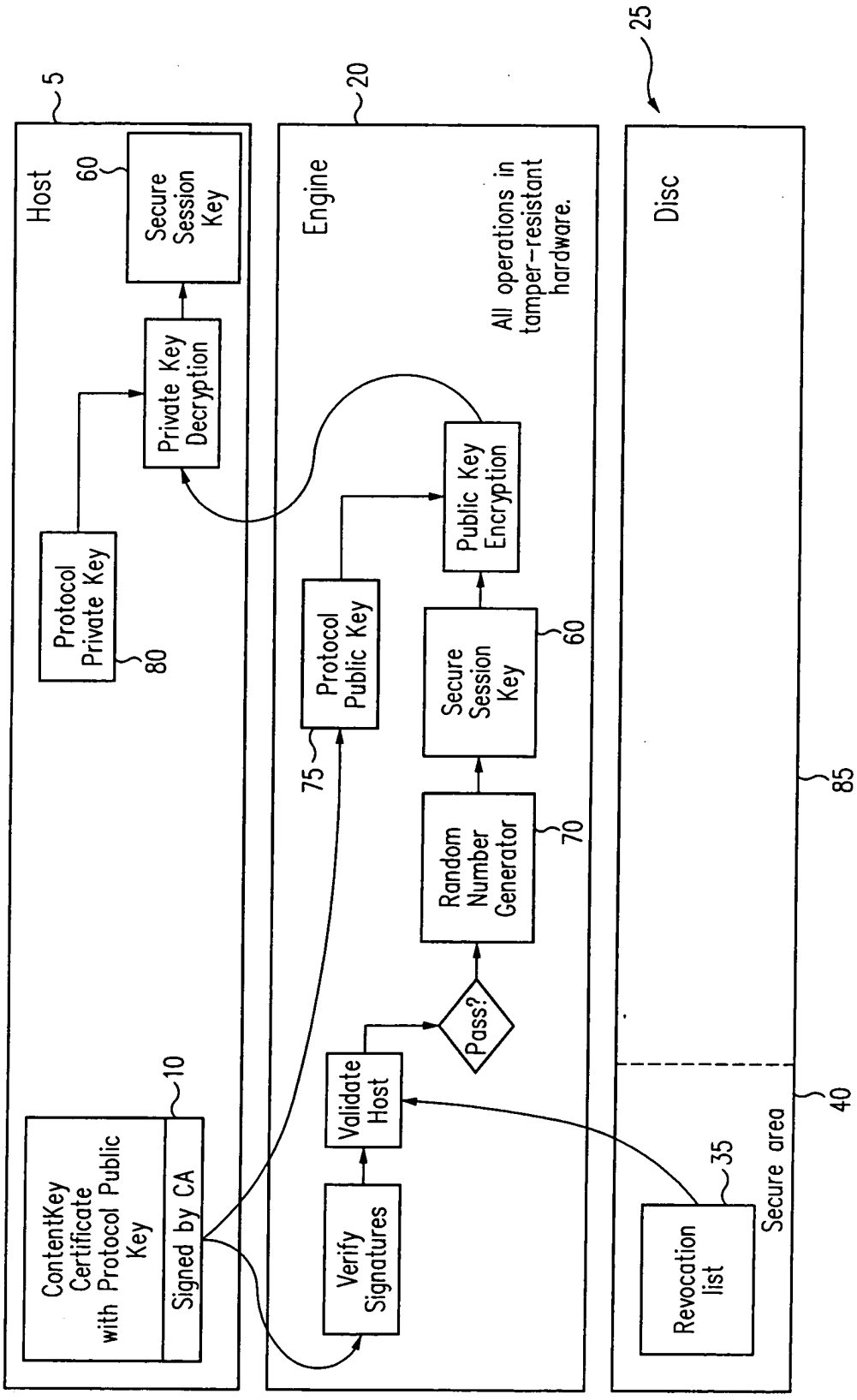

FIG. 1

CK Implementation on HDD Devices

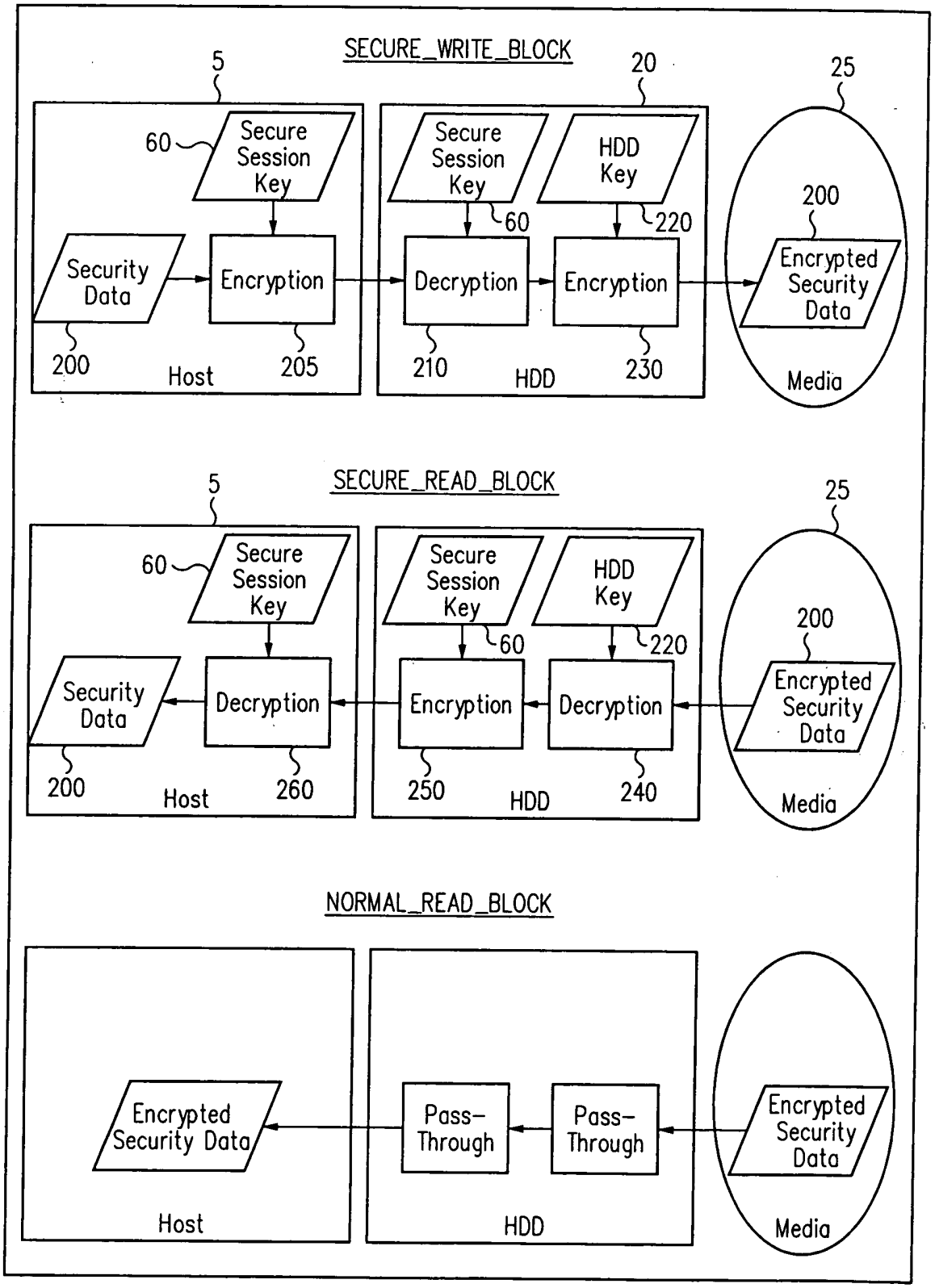

FIG. 2

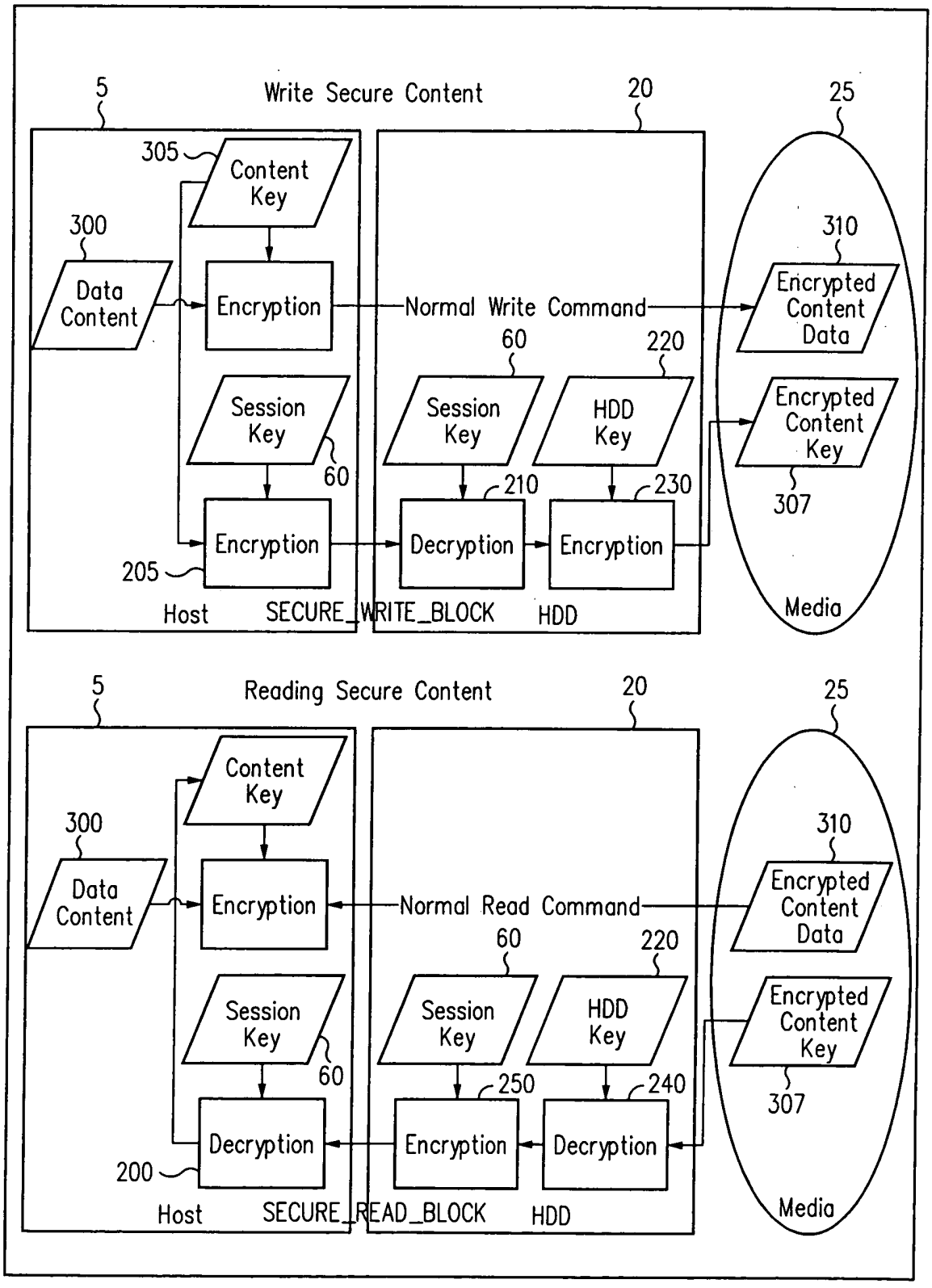
5
Write Secure Content
20
25
305
Content Key
300
Data Content
Encryption
Normal Write Command
310
Encrypted Content Data
60
220
Session Key
HDD Key
Session Key
60
210
230
Encrypted Content Key
307
Encryption
Decryption
Encryption
205
Host
SECURE_WRITE_BLOCK
HDD
Media
5
Reading Secure Content
20
25
Content Key
300
Data Content
Encryption
Normal Read Command
310
Encrypted Content Data
60
220
Session Key
HDD Key
Session Key
60
250
240
Encrypted Content Key
307
Decryption
Encryption
Decryption
200
Host
SECURE_READ_BLOCK
HDD
Media

FIG. 3

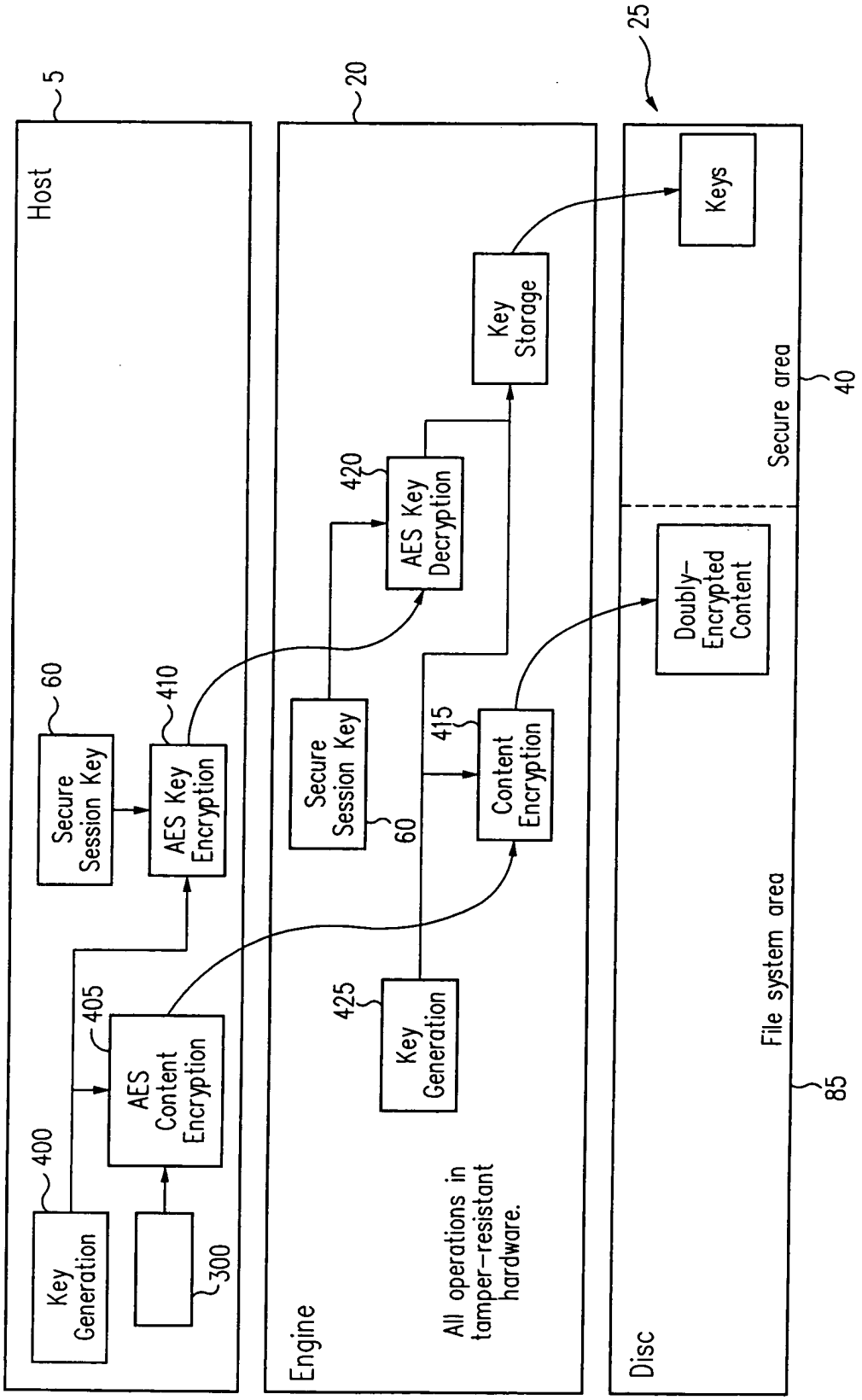
5
Host
20
25
Keys
Key Storage
Secure area
40
420
AES Key Decryption
Doubly-Encrypted Content
60
Secure Session Key
410
AES Key Encryption
415
Content Encryption
Secure Session Key
60
405
AES Content Encryption
425
Key Generation
400
Key Generation
300
All operations in tamper-resistant hardware.
Engine
File system area
85
Disc

FIG. 4

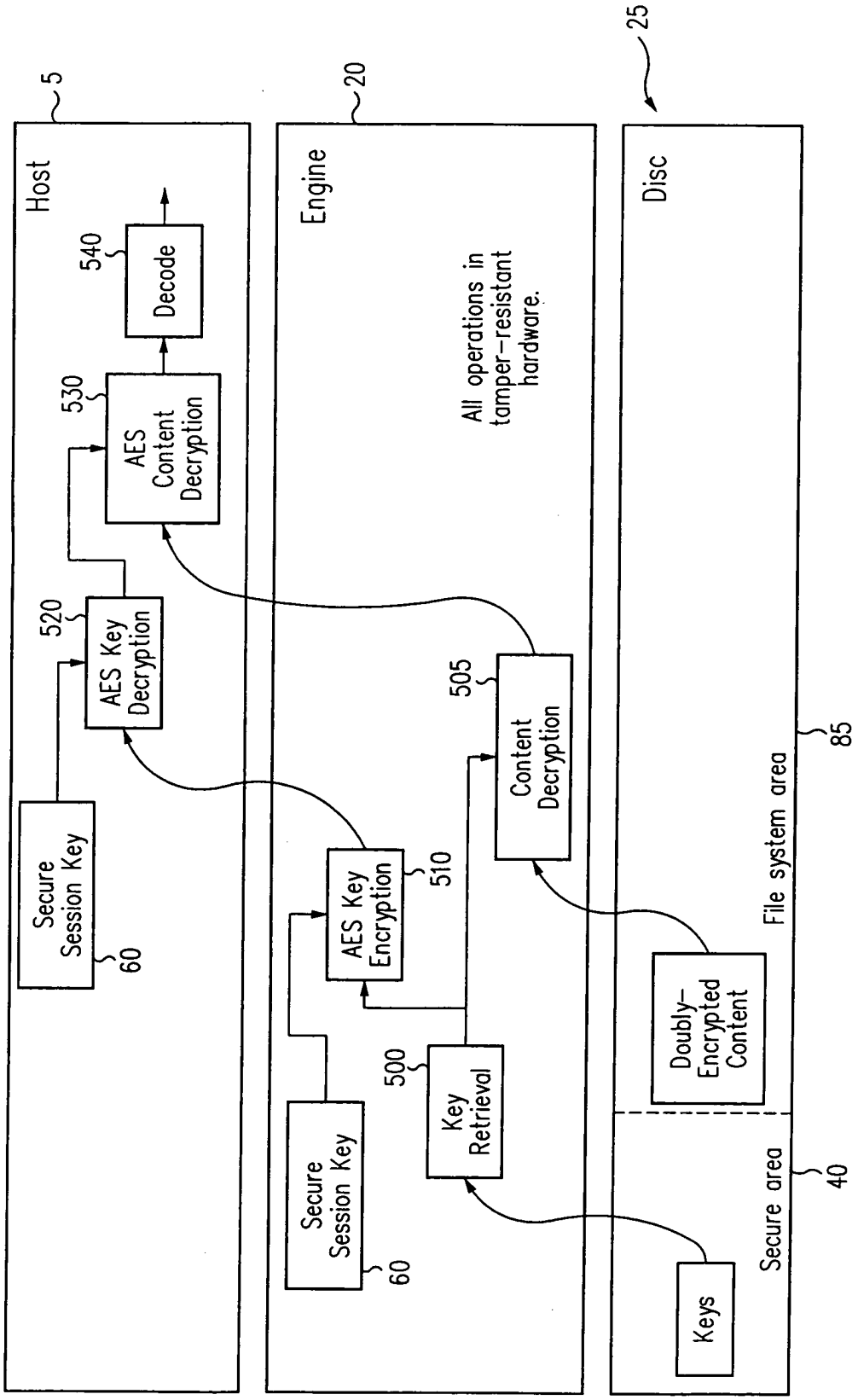
Host
5
Engine
20
Disc
25
All operations in tamper-resistant hardware.
Decode
540
AES Content Decryption
530
AES Key Decryption
520
Secure Session Key
60
AES Key Encryption
510
Content Decryption
505
Key Retrieval
500
Secure Session Key
60
Doubly-Encrypted Content
File system area
85
Keys
Secure area
40

FIG. 5

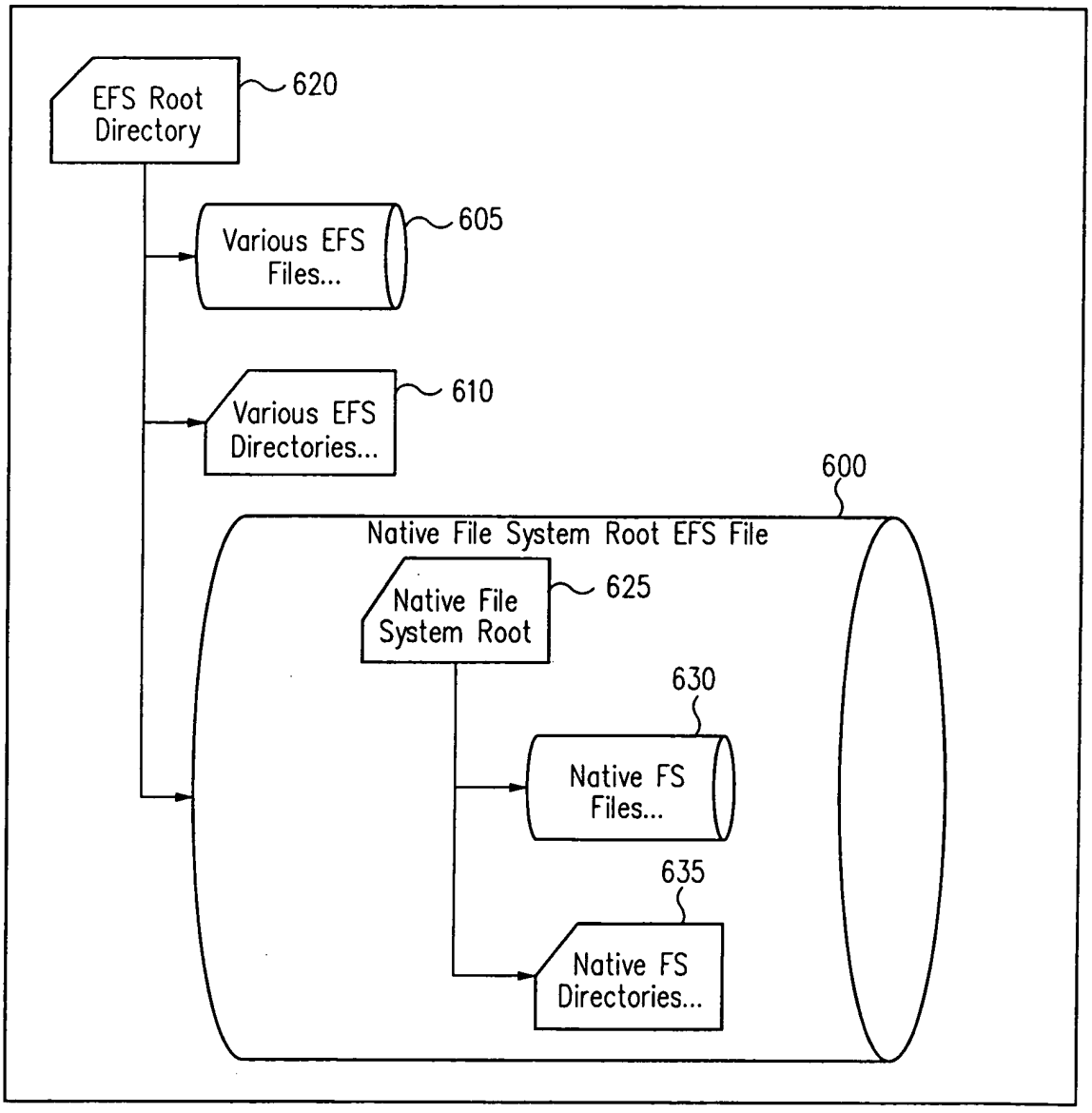
EFS Root Directory
620
Various EFS Files...
605
Various EFS Directories...
610
600
Native File System Root EFS File
Native File System Root
625
630
Native FS Files...
635
Native FS Directories...

FIG. 6